

Web Images Videos Maps News Shopping Gmail more ▼

[Sign in](#)



DES and differential power analysis

Search

[Advanced Search](#)

[Preferences](#)

Web

Results 1 - 10 of about **117,000** for **DES and differential power analysis**. (0.20 seconds)



Show options...

Scholarly articles for **DES and differential power analysis**



DES and differential power analysis - Goubin - Cited by 234

Differential power analysis in the presence of hardware ... - Clavier - Cited by 172

Resistance against **differential power analysis** for ... - Coron - Cited by 407

1. **DES and Differential Power Analysis**

DES and Differential Power Analysis. 163. 2. Replacing some of the critical instructions (in particular the basic assembler ...

www.springerlink.com/index/WNW0V6CC7Q0UX7P1.pdf - [Similar](#)

by L Goubin - 1999 - [Cited by 234](#) - [Related articles](#)

2. Enhanced **DES** Implementation Secure Against High-Order **Differential** ...

Since **Differential Power Analysis** (DPA) on **DES** in smart- L. Goubin and J. Patarin, **DES and Differential Power Analysis** -The Duplication ...

www.springerlink.com/index/64WUG6JP4LT5888G.pdf - [Similar](#)

by J Lv - 2005 - [Cited by 7](#) - [Related articles](#)

3. **DES and Differential Power Analysis** - The "Duplication" Method ...

Paul Kocher recently developed attacks based on the electric consumption of chips that perform cryptographic computations. Among those attacks, the Di ...

citeseer.ist.psu.edu/goubin99des.html - [Similar](#)

4. [PDF] 1 Background 2 Introduction to **Power Analysis**

File Format: PDF/Adobe Acrobat - [View](#)

differential **power analysis**, DPA, SPA, cryptanalysis, **DES**. 1 Background. Attacks that involve multiple parts of a security system are difficult to predict ...

www.cryptography.com/resources/whitepapers/DPA.pdf - [Similar](#)

by P Kocher - 1999 - [Cited by 1642](#) - [Related articles](#) - [All 13 versions](#)

5. [DES and Differential Power Analysis \(The "Duplication" Method\)](#)

Jiqiang Lv, On two **DES** implementations secure against **differential power analysis** in smart-cards, Information and Computation, v.204 n.7, p.1179-1193, ...
portal.acm.org/citation.cfm?id=752372 - [Similar](#)
by L Goubin - 1999 - [Cited by 234](#) - [Related articles](#) - [All 6 versions](#)

6. [On two DES implementations secure against differential power ...](#)

To defend **differential power analysis** attacks, Akkar and Giraud presented a Transformed Masking Method and applied it to **DES** implementation in 2001. ...
linkinghub.elsevier.com/retrieve/pii/S0890540106000484 - [Similar](#)
by J Lv - 2006 - [Cited by 2](#) - [Related articles](#) - [All 5 versions](#)

7. [Welcome to IEEE Xplore 2.0: Advanced DES Algorithm against ...](#)

In this article, the advanced **DES** algorithm against **differential power analysis** (DPA) is provided, based on the original model of DPA. ...
ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4402701 - [Similar](#)
by JHXR B Sheng - 2007 - [Related articles](#)

8. [Differential Power Analysis Attacks to Precharged Busses: a ...](#)

[28] L. Goubin, J. Patarin, "**DES and Differential Power Analysis** (The "Dupli- cation" method)," Proc. of Workshop on Cryptographic Hardware and Embed- ...
doi.ieeecomputersociety.org/10.1109/TDSC.2009.1 - [Similar](#)
by M Alioto

9. [The Risks Digest Volume 19: Issue 80](#)

There is now an initial summary on **Differential Power Analysis** on our ... Make **power** consumption measurements of the last few rounds of 1000 **DES** operations. ...
catless.ncl.ac.uk/Risks/19.80.html - [Similar](#)

10. [DES and differential power analysis: The duplication method](#)

DES and differential power analysis: The duplication method. L GOUBIN, J PATARIN Lecture notes in computer science, 158-172, Springer. ...
cat.inist.fr/?aModele=afficheN&cpsidt=1169116 - [Similar](#)
by L GOUBIN - [Cited by 234](#) - [Related articles](#) - [All 6 versions](#)

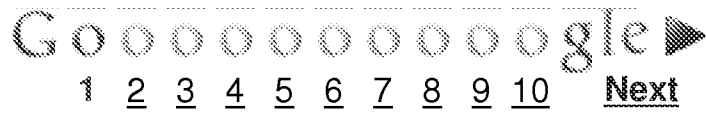
Searches related to: **DES and differential power analysis**

[differential power analysis](#) **kocher**

[differential power attack](#)

[differential fault analysis](#)

[kocher differential power analysis](#)



DES and differential power analysis

Search

[Search within results](#) - [Language Tools](#) - [Search Help](#) - [Dissatisfied? Help us improve](#)
- [Try Google Experimental](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)